CAPSTONE MID-PROJECT PROGRESS SUMMARY: L4 and L5 Autonomous Vehicles Risk Assessment and Best Practices: A Threat Modeling and CIS Security Framework Based Approach

STUDENT TEAM

Jennifer Li, Muskaan Kalra

Advisor

Dr. Terry Thompson

I. What has been completed？

- We have met and discussed the project with Auto-ISAC and reviewed the research papers they suggested to us. We will continue the communication as we progress in the project.
- We have completed seven literature reviews to fully understand the research that has been done until now on level 4 and level 5 autonomous vehicles. Contents of these literature reviews cover from introduction to autonomous vehicles, existing cyber threat studies on Level 1-3 autonomous vehicles, to policies regard to autonomous vehicles from a cybersecurity perspective. The following list contains article titles of the reviews we have done:
  - "Fast-Tracking Advanced Driver Assistance Systems (ADAS) and Autonomous Vehicles Development with Simulation White Paper"
  - "Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicle"
  - "Autonomous Vehicle: Security by Design"
  - "Code of Practice: Automated Vehicle Trialling and the Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles"
  - "Safety and Security Analysis of AEB for L4 Autonomous Vehicle Using STPA"
  - "Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications"
  - "SPY Car Act of 2019"
- We have identified threat surfaces associated with all levels of AVs based on the research papers we have reviewed so far under the Literature Review. More threat surfaces may be added later. Currently, we have studied the following threat surfaces:
  - Front/Rear Short-range Radar and Long-range radar
  - Cloud
  - Ultrasonic sensors and Lidar
  - Software that integrate driver assistance

- V2X Communication
- Cameras
- Infrared sensor and camera
- Advanced Mapping with Geospatial Data

- We decided to do threat modeling using STRIDE as the methodology to implement our security assessment on Level 4 and Level 5 autonomous vehicles. Our thread model approach consists of five major steps as listed below:
  - Identify the valuable assets
  - Create an architecture overview
  - Decompose the architecture of Level 4 and Level 5 autonomous vehicles
  - Identify the threats
  - Document and rate the threats
- We have selected CIS Security Framework to conduct risk assessment for Level 4 and Level 5 autonomous vehicles.
  - Using the basic category, we can lay the minimal requirements for cyber defense readiness in Level 4 and Level 5 autonomous vehicles.
  - With the foundational category, we can suggest best practices for stakeholders within the AV ecosystem to proactively take measures against potential cyber-attacks.
  - With the organizational category, we can identify any regulations or voluntary guidelines towards the people and process.

II. What still needs to be done？

- Document and rate threats
- Perform threat modeling using the Microsoft threat modeling tool
- Implement CIS security controls
- Expand literature review as needed

III. Significant changes to the project proposal

The following significant changes have been made to our project proposal:

- Addition of more significant attack surfaces associated with all levels of autonomous vehicles.
- Perform threat modeling on Level 4 and Level 5 autonomous vehicles in order to conduct a thorough security assessment.
- Use the CIS risk management framework to classify and categorize the challenges associated with autonomous vehicles.

Information Security Institute

CAPSTONE ANNOTATED OUTLINE: L4 and L5 Autonomous Vehicles Risk Assessment and Best Practices: A Threat Modeling and CIS Security Framework Based Approach

STUDENT TEAM

Jennifer Li, Muskaan Kalra

Advisor

Dr. Terry Thompson

Auto-ISAC (Ms. Faye Francy)

TABLE OF CONTENTS

I. ABSTRACT

Abstract will be ready with the final report.

II. INTRODUCTION

Autonomous vehicles ("AV") are a frontier technology that is novel and evolving. Currently, autonomous vehicles are categorized into five levels based on their driving automation capabilities. Level 1 means the automobile contains one single automated system for driver assistance (i.e., monitor speed in cruise control). Level 2 indicates the automobile has partial driving automation such as steering and acceleration. Automobiles that are categorized as Level 3 have conditional driving automation capabilities where the car can make informed decisions themselves based on environmental detection. Level 4 ("L4) is considered as high driving automation where vehicles can operate in the self-driving mode without any human interaction in most circumstances. Level 5 ("L5") vehicles are capable of full driving automation where no human attention is required. Automotive companies are collaborating with technology companies to develop L4 and L5 AVs with ambitious goals to have them on the market within the next five years. Researchers have published studies and recommendations to address AV-related issues, but only a small number of studies have explored the challenges in L4 and L5 AVs. As manufacturers and technology companies around the world race to put L4 and L5 autonomous vehicles in the market, and given the rapid advancements in digital technology that expand the cyber attack surface, it is crucial to study and tackle the issues now for them to be ready for mass-market consumption.

To better understand cyber vulnerabilities and to properly address risks involved in L4 and L5 AVs, our research study serves to inform various stakeholders in the automotive industry of potential threats, risks, and best practices with regards to L4 and L5 AVs. To address these challenges, we partnered with Automotive Information Sharing and Analysis Center ("Auto-ISAC"), an industry-wide forum for companies to collaborate and enhance the cybersecurity posture in the automotive sector. With their extensive resources and knowledge regarding cyber security in autonomous vehicles, Auto-ISAC provides us with external resources, expertise, and guidance as we progress in this research project. Our common goal is to bridge the knowledge gaps related to L4 and L5 autonomous vehicles and cybersecurity.

In this research report, we analyze potential cyber threats, apply the STRIDE threat model that relates to the CIS Security Framework, and provide best practices for automotive industry stakeholders.

III. LITERATURE REVIEW

LR #1: Fast-Tracking Advanced Driver Assistance Systems (ADAS) and Autonomous Vehicles Development with Simulation White Paper

According to SAE (Society of Automated Engineers), there are 6 levels of vehicle automation (0-6) [1]. Levels 0, 1, 2 are the levels in which the human monitors the environment with level 0 offering absolutely no automation on steering, acceleration, deceleration, monitoring driving environment and fallback performance of dynamic driving task to level 2 that offers partial automation where system capabilities are autonomous on some driving modes. Levels 3, 4, 5 are the ones where the cars monitor the environment. Level 3 is conditional automation in which steering, acceleration, deceleration and monitoring driving environment are autonomous without human interaction but fallback control is manually handled and the system capabilities are autonomous only for some driving modes. In level 5 AVs, full automation with all system capabilities fully autonomous are offered in all driving modes. All vehicles beyond level 3 rely on inputs from sensors on the vehicle itself or a combination of self-sensing and sensors on other vehicles or infrastructure. There are lots of challenges in introducing vehicles with full automation. There a risk to human life and property and these AVs require full automation on all geographic areas, weather conditions, traffic conditions, roadway types and all kinds of events or incidents. It is hard because the vehicle needs to be appropriately trained with all these inputs before it is ready to be released.

LR #2: *Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicle*

Weimerskirch and Dominic in a collaboration of MCity Working Group and University of Michigan [2], wrote about identifying and analyzing cybersecurity threats to automated vehicles. They defined a threat model which took into account various scenarios that attackers might be in while hacking into a vehicle. The attack methods also followed the STRIDE classification developed by Microsoft. Further, they went on to designing a threat matrix for automated parking for different attack scenarios, attack potential (system withstand and attacker capability), motivation of the attacker, impact to stakeholders and result vector.

LR #3: *Autonomous Vehicle: Security by Design*

According to Chattopadhyay and Lam 2018 [3], level 4 AVs have system controlled environment monitoring, steering cruise and some driving modes are also system controlled. The only thing human controlled is fallback control (act in cases of emergencies). While, in level 4 AVs, there is full automation for environmental monitoring, steering cruise, fallback control as well as all driving modes are fully autonomous. The higher the degree of automation, the greater the risks. They explore the security-by-design framework for AVs and also explore the technical challenges faced by AV security. They go on to describe cyber-physical systems (CPS) attacks on sensors and actuators like - sensor spoof, DoS, authentication failure, etc. They discuss the security-by-design of AV as a CPS, by identifying and addressing the security objectives within this socio-technical framework. They further also describe the AV security model, Security Objectives and Requirements of AV, Safety Standards for AV, adversarial models for AV security and System Security Model for AV.

LR #4: *UK Code of Practice: Automated Vehicle Trialling and The key principles of vehicle cyber security for connected and automated vehicles*

The UK government plans to have self-driving cars on its roads by 2021. The Centre for Connected and Autonomous Vehicles released a code of practice for automated vehicle trialling [6] with the following legal requirements: (1) A driver is present, in or out of the vehicle, who is ready, able, and willing to resume control of the vehicle; (2) The vehicle is roadworthy; and (3) Appropriate insurance in place. The code of practice also states cyber security challenges faced by autonomous vehicles. Further, the UK government has a document called “Key Principles of Cyber Security for Connected and Automated Vehicles” [4] which is a guidance document for AV cybersecurity. They also have a BSi PAS 1885 which are specifications for fundamental principles of automotive cyber security. There are various laws and principles listed in these documents pertaining to incident response, data storage, product aftercare, supply chain, defense-in-depth approach and response actions in case important systems fail. As of now, in the US, four states (California, Nevada, Florida and the District of Columbia) have passed laws allowing the testing of highly automated vehicles. In Level 4 and Level 5 AVs, there is a need to have systems resilient to cyber attacks and having the AVs trained appropriately in cases of defenses or sensor failures. There should also be appropriate security management throughout the lifetime of the vehicle. There is also a need for collaboration from suppliers, contractors and third parties to enhance vehicle security.

LR #5: *Safety and security analysis of AEB for L4 autonomous vehicle using STPA*

This paper is about how the System Theoretic Process Analysis ("STPA") can be applied to an Automated Emergency Braking ("AEB") system to promote safety and mitigate vulnerabilities. [5]

As background, STPA comprises of four main elements: (1) defining the scope of the analysis, (2) developing control structure diagram, (3) identifying unsafe control actions, and (4) identifying how each unsafe control action could occur. The bulk of this paper is about applying the STPA framework to the AEB system, which involves identifying potential threats to a vehicle and taking prophylactic measures to reduce the probability of a collision (by slowing the vehicle down before it gets too near to other objects).

First, the authors define the scope of the analysis to cover a "functional safety analysis for AEB for an AV using vehicle state and environmental data analysis to contribute to the safety of the passengers and the environment." This operates on several assumptions on accidents (e.g., situations where the AV collides with objects or its passengers are injured), hazards (e.g., failure of the AV to maintain a proper distance from other objects or from a prohibited area) and high-level safety constraints.

Second, the authors develop a control structure diagram.

Third, the authors identify unsafe control actions and try to develop corresponding safety constraints. For instance, an unsafe control action might be where the AEB does not provide braking force command when the AV falls within a critical distance of a potential risk. The corresponding safety constraint is thus for the AEB to provide that BFC once the AV approaches the critical distance.

Fourth, the authors identify how each unsafe control action could occur. This involves developing scenarios using the unsafe control actions ("UCA"), and identifying causal factors corresponding to each scenario. For instance, a controller might suffer from a UCA (e.g., inadequate or incorrect information) due to various reasons (e.g., spoofing, component failures, or other problems).

LR #6: *Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications*

In this paper, author Araz Taeihagh describes the cybersecurity risks, as well as the privacy concerns introduced by AVs with a focus on implementing AVs for smart and sustainable cities.[6] By analyzing various regulation and voluntary guidelines by federal

governments in the US, the UK, China, Singapore, the EU, and etc., he further addresses AV-related risks in depth. He states the cybersecurity of AVs is essential for economic sustainability, safety, and social stability. The vulnerabilities we face in cybersecurity stem from the use of ICTs and their interactions with cyberspace. The risk of bad actors hacking communication networks (i.e., wireless networks) can undermine safety-critical functions of the AV system, and expose the critical infrastructure supporting the system to related cyber threats. In addition, the current automotive industry standards "lacks sufficient coverage for the breadth of cybersecurity risks faced by AV" and we need to ensure intensive collaboration between the stakeholders within the AV ecosystem to work on both the physical and cyber safety for AV users.

LR #7: *SPY Car Act of 2019*

On July 18, 2019, Senator Edward Markey from Massachusetts and Senator Richard Blumenthal from Connecticut proposed the bill -- Security and Privacy in Your Car Act ("SPY Car Act"). This bill creates a cybersecurity standard that focus on cybersecurity threats and protect drivers' privacy affect stakeholders across the ecosystem (i.e., manufactures, suppliers). For instance, manufacturers are required to provide to its consumers a comprehensive and detailed driving data that vehicle collects and transmits. Consumers also have the option to opt out of this data collection. As a whole, this bill requires all cars that are sold in the U.S. must have appropriate measures to protect all threat entry points. All data generated and transmitted during the drive must be secured and all the AVs be equipped with "capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle." [7] This bill also requires NHTSA and the FTC to propose rules for these standards within the next year and a half and to promulgate final rules within three years.

IV. PROBLEM DEFINITION

As manufacturers make ambitious plans to accelerate the introduction of these vehicles into the market, the automotive industry, Congress, insurance companies, and other stakeholders in the automotive industry must work together to reduce the risks to the driving public. This is a huge problem. In this capstone project, we hope to advance understanding of cyber vulnerabilities and risks related to Level 4 and 5 AVs by identifying and prioritizing the cyber risks, analyze these risks, and apply the Center for Internet Security Framework to recommend potential best practices to all stakeholders

We will be tackling the problems mentioned above with mentorship from Auto-ISAC members to identify cyber-attack surfaces and the threat model throughout the project.

- Using the research done by the Center for Automotive Embedded Systems Security
- Research paper: “Risk Assessment for Cooperative Automated Driving” that includes potential frameworks like EVITA, NHTSA and others.
- Miller and Valasek, “Securing Self-Driving Cars (one company at a time)
- UC, San Diego and University of Washington’s research on “Comprehensive Experimental Analyses of Automotive Attack Surfaces”

V. RESEARCH DONE SO FAR

A. Attack Surfaces

- Attack Surface 1: Front/Rear Short-range Radar and Long-range radar
    - Automotive radar sensors are of two categories - short-range radar (SRR) and long-range radar (LRR). A combination of these radars provides valuable data for advanced driver assistance systems. The applications of short range radars includes but not limited to (1) ACC support with Stop and Go functionality, (2) collision warning, (3) collision mitigation, (4) blind spot monitoring, (5) parking aid (forward and reverse), (6) lane change assistant, and (7) rear crash collision warning.
    - Though most frequently used as part of features like parking assistance and blind-spot detection, they have the capability to detect objects at much greater range – several hundred feet in fact.
    - Radar sensors are excellent at detecting objects, but they’re also excellent for backing up other sensors. For instance, a front-facing camera can’t see through heavy weather. On the other hand, radar sensors can easily penetrate fog and snow, and can alert a driver about conditions obscured by poor conditions.
    - According to a group of researchers at the University of South Carolina, China’s Zhejiang University and the Chinese security firm Qihoo 360 [10], only their radar attacks might have the potential to cause a high-speed collision. They used two pieces of radio equipment—a $90,000 signal generator from Keysight Technologies and a VDI frequency multiplier to precisely jam the radio signals given by Tesla's radar sensor, located under its front grill and made them bounce off of objects to determine their position. The researchers placed the equipment on a cart in front of the Tesla to simulate another vehicle. "When there’s jamming, the 'car' disappears, and there’s no warning," said one of them. Thus, the radar is

a huge attack surface for autonomous vehicles and has the potential of being attacked.

- Attack Surface 2: Cloud
    - Connecting a smartphone can pose to be a risk to an autonomous vehicle. Interacting with an unfamiliar device can be a threat. The phone may be sending and receiving data from the cloud and on any kind of hack to the data center, the vehicle would also come in contact with the compromised data center and be prone to cyber attacks [12].
    - There are also security and privacy concerns related to the cloud when multiple users access the cloud and share the same resources [13].

- Attack Surface 3: Ultrasonic Sensors and Lidar
    - Park assist is the feature that vehicles use for parking in tight spots. Park assist makes use of ultrasonic sensors to calculate how far an obstacle is and calculates the driving angle to assist the driver in parking.
    - Lidar sensors are used by cars to detect objects and are usually located on the roof of the car. Low power lasers can be used to hack the lidar by tricking the lidar into detecting fake echoes of objects such as people or cars [11].
    - Spoofed objects can be placed in the path of autonomous vehicles by hacking these sensors which can cause serious damage.

- Attack Surface 4: Software that integrate driver assistance functions and algorithms for every scenario
    - These are algorithms related to decisions, planning and control in scenarios involving autonomous vehicles and monitoring them for safety, cooperation and human compatible traffic automation. The connected vehicle and connected infrastructure approach require available data transmission frequencies, low-latency, trusted, secure and fail-safe data transmission protocols. The advanced driver assistance system (ADAS) has the ability to recognize other vehicles, pedestrians, road signs, road markings, trees, buildings, traffic lights and a lot of other things that a driver encounters every day. Another hardship is identifying these in poor driving conditions such as darkness of the night, rain and snow.
    - These ADAS areas are mostly used: (1) Driving Scenario System Simulation; (2) Software and Algorithm Modeling and Development; (3) Functional Safety Analysis; (4) Sensor Performance Simulation; (5) Electronics Hardware Simulation and (6) Semiconductor Simulation.

    - Rule-based computer algorithms are insufficient for this. Instead, neural-networks and machine-learning methods need to be used. In these methods the computer is trained. But driving is such a complex task that an immense amount of training will be needed to make a computer drive as safely and reliably as an average human. An autonomous vehicle will need to be driven through billions of miles of road tests to train its artificial intelligence to the same level of safety and reliability as a human driver, according to researchers [8].

- Attack Surface 5: V2X Communication
    - The meaning of “V2X’ is Vehicle to things. Two types of communication falls under this category, (1) V2V and (2) V2I. V2V denotes Vehicle to Vehicle communication. V2I denotes Vehicle to Infrastructure communication. V2X is still pre-deployment, and V2X doesn’t cover the wireless standards. A lot of folks focus on V2X in the AV context. While it may help, a more fundamental question is what role it actually will play given the deployment rates won’t have it widely adopted during early AV deployment.

- Attack Surface 6: Cameras
    - Two main cameras used in AV are (1) monoscopic and (2) stereoscopic cameras. They are often used to detect “lane detection, traffic sign recognition, headlight detection, obstacle detection, and etc.” [14] This component can potentially create an entry point for bad actors to introduce safe concerns in the real world, such as “false detection or not detection of objects.”

- Attack Surface 7: Infrared Sensor and Camera
    - Infrared sensor measures infrared light of objects and detect motions. In autonomous vehicles, they are often used to detect people and objects in various challenging conditions. [16]

- Attack Surface 8: Geographic Information Science
    - Geographic Information Science (GIS) play crucial roles in autonomous vehicles. While sensors, radars, and computer vision algorithms integrates to provide capabilities for cars that follow traffic laws, GIS are used to provide extensive routing data and detailed maps that allow a vehicle to proceed. There are three main trends that makes GIS important, yet with cybersecurity concerns. Firstly, GIS has the ability to collect and analyze

real-time data. This allows the GIS to make smart driving decisions when facing time-sensitive decisions. Secondly, GIS generates and transmit consumer-facing data. Thirdly, GIS integrates heavily with artificial intelligence that helps to analyze data, such as drivers can share data related to traffic that can help researched to identify traffic patterns. While this amazing technology can help in various aspects of the automotive industry, its abilities and the amount of data generates also makes it a lucrative target for attackers.

VI. TECHNICAL SOLUTION, DESIGN, and ANALYSIS

We plan to use threat modeling as the technique to implement our security assessment on Level 4 and Level 5 autonomous vehicles. A potential tool we may use is the Microsoft threat modeling tool to improve process efficiency. The following is our planned threat modeling process:

1. Identify the valuable assets
   In this step, we identify the assets we need to protect in Level 4 and Level 5 autonomous vehicles.
2. Create an architecture overview
   In this step, we use tables and tool (i.e., Microsoft threat modeling tool) to document the architecture of Level 4 and Level 5 autonomous vehicles. Based on the study of existing attack surfaces, we can identify the technology used and list out the corresponding architecture components related to the entry points. An Architecture flow diagram may be produced at this step.
3. Decompose the architecture of Level 4 and Level 5 autonomous vehicles
   In this step, we analyse the trust boundaries and threat entry points to create a security profile file.The purpose of the security profile is to uncover vulnerabilities in the design, implementation, or deployment configuration of Level 4 and Level 5 autonomous vehicles.
4. Identify the threats
   With knowledge of the architecture and potential vulnerabilities, we can identify threats that could affect Level 4 and Level 5 autonomous vehicles. We can use the attack tree, attack patterns and/or STRIDE based threat to identify threats.
5. Document and rate the threats
   In this step, we create threat templates that describe the threats, threat targets, risks, attack techniques, and countermeasures. We can then rate and prioritize threats with the DREAD method.

VII. EXPERIMENTATION, EVALUATION, and RESULT ANALYSIS

During this step, we plan use the CIS Security Framework to build security for Level 4 and Level 5 autonomous vehicles. With the list of well-defined security controls, CIS allows us to prioritize the set of controls that can be implemented corresponding to the threat models we prioritized in Section V. We can use the three distinct categories of CIS Controls (basic, foundational, organizational) to perform our analysis. Using the basic category, we can lay the minimal requirements for cyber defense readiness in Level 4 and Level 5 autonomous vehicles. With the foundational category, we can suggest best practices for stakeholders within the AV ecosystem to proactively take measures against potential cyber-attacks. With the organizational category, we can identify any regulations or voluntary guidelines towards the people and process.

VIII. CONCLUSION

Automotive companies and technology companies are working extensively to reach the ultimate level of autonomous vehicles in the next five years. While we are excited to see the possibilities AVs can bring to our social welfare, we focus our research study on advance the thinking about cyber vulnerabilities and risks in L4 and L5 AVs, as well as ways to address them using an established cyber risk management framework.

[...Then go onto to talk about other, interconnected things like the AV infrastructure, etc.]

[...] Due to the interrelationship between autonomous vehicles and their surrounding infrastructure, these incidents involve not just the vehicles themselves, but also the whole ecosystem that will be developed to support such vehicles. This is why every stakeholder within the AV ecosystem must collaborate and work together to ensure a safer future. In our research…[coming soon]

[...] Potential Impacts of Technology Advancements
(Brainstorming ideas, feedbacks are welcomed! Thoughts: maybe we can talk about how technology advancements in the next few years can impact the above attack surfaces? or in L4+L5 in general? Or use this as a way to list potential threats to the L4+L5?)

- Artificial Intelligence
- Internet of Things
- 5G

IX. REFERENCES

1. Sandeep Sovani, “Fast-Tracking Advanced Driver Assistance Systems (ADAS) and Autonomous Vehicles Development with Simulation White Paper”, http://pdfs.semanticscholar.org/32bf/acb92e2c62752d207cbea6bfa26d48d4ce93.pdf
2. Mcity by University of Michigan, “Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles”, https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf
3. Anupam Chattopadhyay, “Autonomous Vehicle: Security by Design”, https://arxiv.org/pdf/1810.00545.pdf
4. U.K. Government, “Code of Practice Automated Vehicle Trialling”, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776511/code-of-practice-automated-vehicle-trialling.pdf
5. Shafali, “Safety and security analysis of AEB for L4 autonomous vehicle using STPA,” http://drops.dagstuhl.de/opus/volltexte/2019/10338/pdf/OASIcs-ASD-2019-5.pdf
6. Taeihagh, A. Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. Energies (19961073), [s. l.], v. 11, n. 5, p. 1062, 2018. Disponível em: <http://search.ebscohost.com.proxy1.library.jhu.edu/login.aspx?direct=true&db=asn&AN=132396988&site=ehost-live&scope=site>. Acesso em: 20 out. 2019.’
7. U.K. Government, “Principles of Cybersecurity for Connected and Automated Vehicles”, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles
8. Congress, “S.2182 - SPY Car Act of 2019”, https://www.congress.gov/bill/116th-congress/senate-bill/2182/texthttps://www.natlawreview.com/article/senators-reintroduce-cybersecurity-legislation-cars-and-planes
9. International Transport Forum, “Automated and Autonomous Driving”, https://cyberlaw.stanford.edu/files/publication/files/15CPB_AutonomousDriving.pdf
10. Jalopnik, “Hackers Show That Tesla Autonomous Sensors Can Be Fooled, But It's All A Bit Stupid”, https://jalopnik.com/hackers-show-that-tesla-autonomous-sensors-can-be-foole-1784825823
11. Rosique, Lorente, Fernandez and Padilla, “A Systematic Review of Perception System and Simulators for Autonomous Vehicles Research”,

https://www.researchgate.net/publication/330900887_A_Systematic_Review_of_Perception_System_and_Simulators_for_Autonomous_Vehicles_Research
12. Amara, Chebrolu, R and Kp, “A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities”, https://www.researchgate.net/publication/328189443
13. Vasudavan, Shanmugam and Ahmada, “The adoption of cloud computing in autonomous vehicle”, https://www.sciencepubco.com/index.php/ijet/article/view/15480/6417
14. Amara Dinesh Kumar, “A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities”, https://openreview.net/pdf?id=Byl_m_Z4Ym
15. Raj Gautam Dutta, “Security of Autonomous Systems under Physical Attacks: With application to Self-Driving Cars”, http://stars.library.ucf.edu/cgi/viewcontent.cgi?article=6957&context=etd
16. Jonathan Petit, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”, https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf
17. Wired, “Let the Robot Drive: The Autonomous Car of the Future Is Here”, http://www.wired.com/2012/01/ff_autonomouscars/all/

X. APPENDICES

As the project progresses, we may add tables, matrices, and definitions of words used.